Measures for the Security Protection and Administration of International Networking of Computer Information Networks of China (the PRC)

Dan Young Business Consultancy — www.danyoungcpa.com

Unofficial English translation prepared for reference only. The official Chinese text prevails.

Contents

Table of Contents 1

Chapter I — General Provisions 1

Chapter II — Security Protection Responsibilities 2

Chapter III — Security Supervision 3

Chapter IV — Legal Liability 3

Chapter V — Supplementary Provisions 4

Approved by the State Council on December 11, 1997; promulgated by Order No. 33 of the Ministry of Public Security on December 16, 1997; revised in accordance with the Decision of the State Council on Abolishing and Amending Certain Administrative Regulations (Decree No. 588) of January 8, 2011

Table of Contents

- Chapter I — General Provisions
- Chapter II — Security Protection Responsibilities
- Chapter III — Security Supervision
- Chapter IV — Legal Liability
- Chapter V — Supplementary Provisions

Chapter I — General Provisions

Article 1 — These Measures are formulated in accordance with the Regulations of the People's Republic of China on the Security Protection of Computer Information Systems, the Interim Provisions of the People's Republic of China on the Administration of International Networking of Computer Information Networks, and other laws and administrative regulations, for the purpose of strengthening the security protection of the international networking of computer information networks and maintaining public order and social stability.

Article 2 — These Measures shall apply to the administration of the security protection of the international networking of computer information networks within the territory of the People's Republic of China.

Article 3 — The computer administration and supervision organ of the Ministry of Public Security shall be responsible for the administration of the security protection of the international networking of computer information networks. The computer administration and supervision organs of the public security organs shall protect the public security of the international networking of computer information networks and safeguard the lawful rights and interests of units and individuals engaged in international networking business and the public interest.

Source: https://www.danyoungcpa.com/measures-security-protection-international-networking-china/

Article 4 — No unit or individual may use international networking to endanger State security or divulge State secrets, infringe upon the interests of the State, society and collectives or the lawful rights and interests of citizens, or engage in illegal or criminal activities.

Article 5 — No unit or individual may use international networking to produce, reproduce, access or disseminate the following information: (1) information inciting resistance to or disruption of the implementation of the Constitution, laws and administrative regulations; (2) information inciting the subversion of State power and the overthrow of the socialist system; (3) information inciting the division of the State and undermining national unity; (4) information inciting ethnic hatred or ethnic discrimination and undermining ethnic unity; (5) information fabricating or distorting facts, spreading rumors and disturbing social order; (6) information propagating feudal superstition, obscenity, pornography, gambling, violence, murder or terror, or instigating crime; (7) information openly insulting others or fabricating facts to slander others; (8) information harming the reputation of State organs; or (9) other information violating the Constitution, laws and administrative regulations.

Article 6 — No unit or individual may engage in the following activities endangering the security of computer information networks: (1) entering a computer information network or using the resources of a computer information network without permission; (2) deleting, modifying or adding to the functions of a computer information network without permission; (3) deleting, modifying or adding to data and applications stored, processed or transmitted in a computer information network without permission; (4) deliberately producing or disseminating destructive programs such as computer viruses; or (5) other activities endangering the security of computer information networks.

Article 7 — The freedom and confidentiality of correspondence of users shall be protected by law. No unit or individual may, in violation of the provisions of the law, use international networking to infringe upon the freedom and confidentiality of correspondence of users.

Chapter II — Security Protection Responsibilities

Article 8 — Units and individuals engaged in international networking business shall accept the security supervision, inspection and guidance of the public security organs, truthfully provide the public security organs with the information, materials and data files related to security protection, and assist the public security organs in investigating and handling illegal and criminal acts committed through the international networking of computer information networks.

Article 9 — The units providing international gateway channels, and the competent departments or units in charge of interconnection units, shall be responsible for the security protection and administration of the international gateway channels and their affiliated interconnection networks in accordance with the law and the relevant provisions of the State.

Article 10 — Interconnection units, access units, and legal persons and other organizations using the international networking of computer information networks shall perform the following security protection duties: (1) taking charge of the security protection and administration of their own networks and establishing and improving security protection management systems; (2) implementing technical measures for security protection and ensuring the operational security and information security of their own networks; (3) taking charge of security education and training for the users of their own networks; (4) registering the units and individuals that commission the publication of information, and examining the content of the information provided in accordance with Article 5 of these Measures; (5) establishing user registration and information management systems for the electronic bulletin systems of computer information networks; (6) where any of the circumstances listed in Articles 4, 5, 6 and 7 of these Measures is discovered, preserving the relevant original records and reporting to the local public security organ within 24 hours; and (7) deleting, in accordance with the relevant provisions of the State, the addresses and directories containing the content prescribed in Article 5 of these Measures from their own networks or shutting down the servers.

Source: https://www.danyoungcpa.com/measures-security-protection-international-networking-china/

Article 11 — When a user completes the formalities for network access at an access unit, the user shall fill in a user filing form. The filing form shall be supervised and produced by the Ministry of Public Security.

Article 12 — Interconnection units, access units, and legal persons and other organizations using the international networking of computer information networks (including units connected across provinces, autonomous regions and municipalities directly under the Central Government and their affiliated branch organs) shall complete the filing formalities with the receiving organ designated by the public security organ of the people's government of the province, autonomous region or municipality directly under the Central Government at their locality within 30 days from the date the network is officially connected. The units listed in the preceding paragraph shall be responsible for reporting the access units and users connected to their own networks to the local public security organ for filing, and shall promptly report the changes in the access units and users of their own networks.

Article 13 — Registrants using public accounts shall strengthen the management of public accounts and establish a registration system for the use of accounts. User accounts shall not be lent or transferred.

Article 14 — When units involved in important fields such as State affairs, economic construction, national defense construction and advanced science and technology complete the filing formalities, they shall present the examination and approval certificate of their competent administrative department. The computer information networks of the units listed in the preceding paragraph that are internationally networked shall adopt corresponding security protection measures.

Chapter III — Security Supervision

Article 15 — The public security departments (bureaus) of provinces, autonomous regions and municipalities directly under the Central Government, and the public security bureaus of prefectures (cities) and counties (cities), shall have corresponding organs responsible for the security protection and administration of international networking.

Article 16 — The computer administration and supervision organs of the public security organs shall keep abreast of the filing situation of interconnection units, access units and users, establish filing archives, conduct filing statistics, and report level by level in accordance with the relevant provisions of the State.

Article 17 — The computer administration and supervision organs of the public security organs shall urge interconnection units, access units and relevant users to establish and improve security protection management systems, and supervise and inspect the implementation of network security protection administration and technical measures. When the computer administration and supervision organs of the public security organs organize security inspections, the relevant units shall send personnel to participate. The computer administration and supervision organs of the public security organs shall put forward improvement opinions on the problems discovered in security inspections, make detailed records, and keep them on file for future reference.

Article 18 — Where the computer administration and supervision organs of the public security organs discover addresses, directories or servers containing the content listed in Article 5 of these Measures, they shall notify the relevant units to shut them down or delete them.

Article 19 — The computer administration and supervision organs of the public security organs shall be responsible for tracking, investigating and handling illegal acts conducted through computer information networks and criminal cases against computer information networks, and shall, in accordance with the relevant provisions of the State, transfer illegal and criminal acts violating Articles 4 and 7 of these Measures to the relevant departments or judicial organs for handling.

Chapter IV — Legal Liability

Article 20 — Where a party, in violation of laws and administrative regulations, commits any of the acts listed in Articles 5 and 6 of these Measures, the public security organ shall give it a warning and, where there are illegal gains, confiscate the illegal gains; a fine of not more than RMB 5,000 may be imposed in addition on an individual, and a fine of not more than RMB 15,000 may be imposed in addition on a unit; where the circumstances are serious, a penalty of discontinuing networking and suspending the operation for rectification for not more than six months may also be imposed, and where necessary, the original license-issuing or examination and approval organ may be advised to revoke the business license or cancel the networking qualification; where the act constitutes a violation of public security administration, it shall be punished in accordance with the provisions of the Law on Penalties for Administration of Public Security; and where the act constitutes a crime, criminal responsibility shall be investigated in accordance with law.

Article 21 — Where a party commits any of the following acts, the public security organ shall order it to make corrections within a prescribed time limit and give it a warning, and where there are illegal gains, confiscate the illegal gains; where it fails to make corrections within the prescribed time limit, a fine of not more than RMB 5,000 may be imposed in addition on the persons in charge and other directly responsible persons of the unit, and a fine of not more than RMB 15,000 may be imposed in addition on the unit; where the circumstances are serious, a penalty of discontinuing networking and suspending the operation for rectification for not more than six months may also be imposed, and where necessary, the original license-issuing or examination and approval organ may be advised to revoke the business license or cancel the networking qualification: (1) failing to establish a security protection management system; (2) failing to adopt technical measures for security protection; (3) failing to conduct security education and training for network users; (4) failing to provide the information, materials and data files required for security protection administration, or providing untrue content; (5) failing to examine the content of information commissioned for publication or failing to register the commissioning units and individuals; (6) failing to establish user registration and information management systems for electronic bulletin systems; (7) failing to delete network addresses and directories or shut down servers in accordance with the relevant provisions of the State; (8) failing to establish a registration system for the use of public accounts; or (9) lending or transferring user accounts.

Article 22 — Violations of Articles 4 and 7 of these Measures shall be punished in accordance with the relevant laws and regulations.

Article 23 — Where a party violates Articles 11 and 12 of these Measures by failing to perform the filing duties, the public security organ shall give it a warning or impose a penalty of suspending the operation for rectification for not more than six months.

Chapter V — Supplementary Provisions

Article 24 — The security protection and administration of computer information networks connected with the Hong Kong Special Administrative Region and the Taiwan and Macao regions shall be carried out by reference to these Measures.

Article 25 — These Measures shall be implemented as of December 30, 1997.

Disclaimer: This document is an unofficial English translation of a Chinese administrative regulation, prepared for general informational and reference purposes only. It is not an official translation and has no legal effect. While every effort has been made to ensure accuracy, the official Chinese text is the sole authoritative version. Readers should consult qualified legal counsel before relying on this translation for any legal matter.